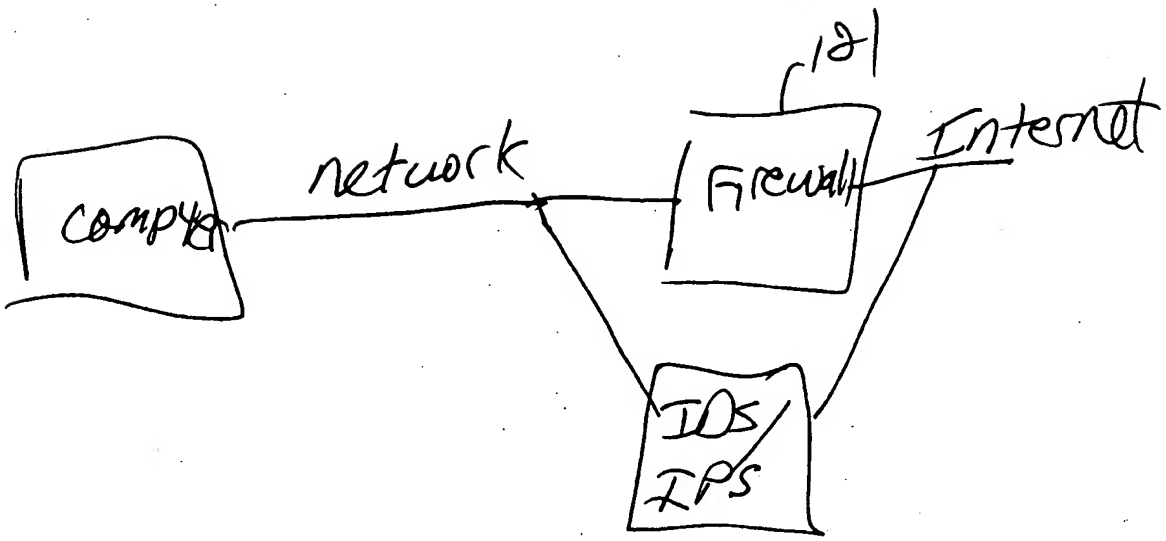

FIG 1

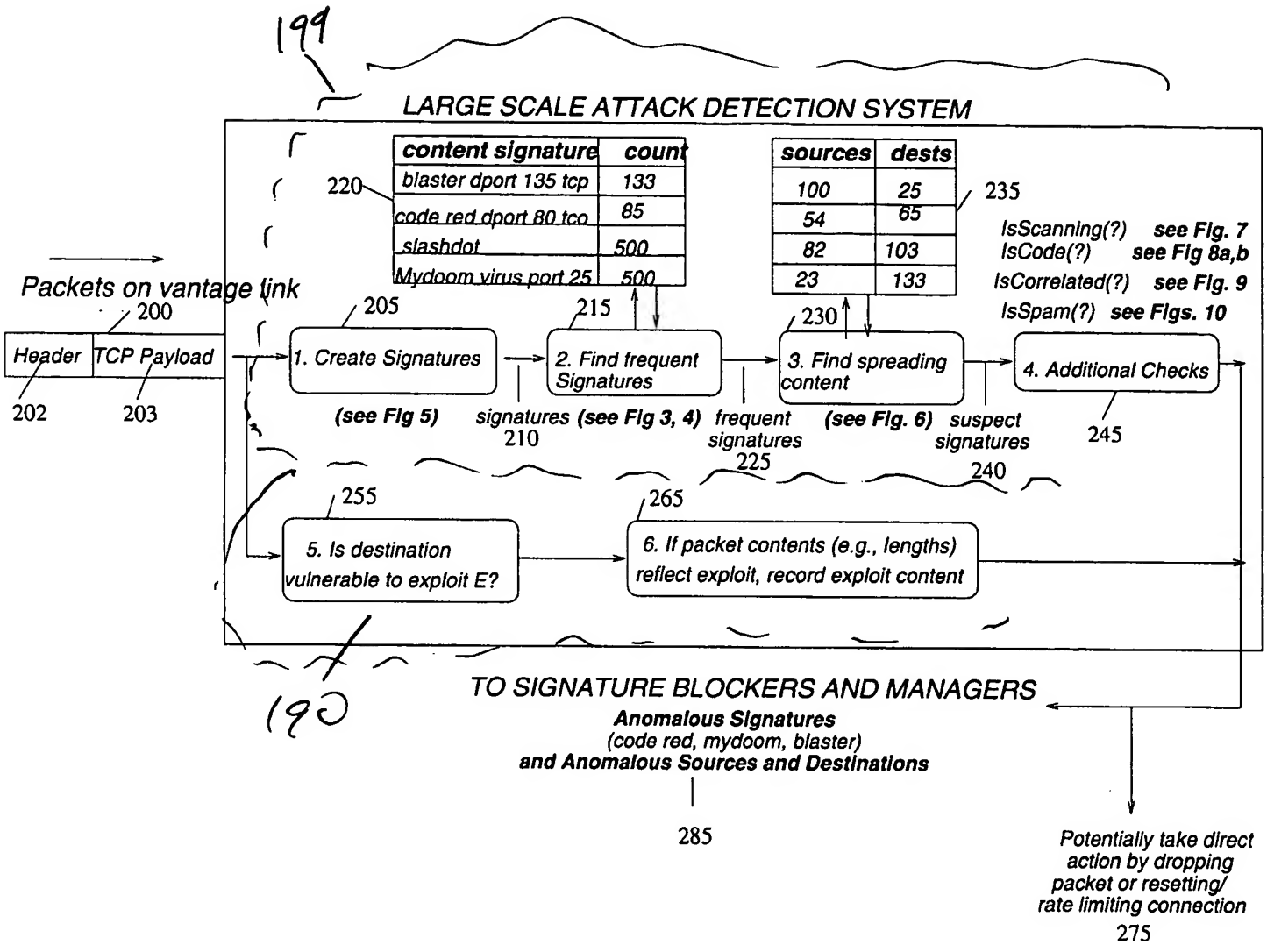

Figure 2: Large Scale Indtrusion Detection System

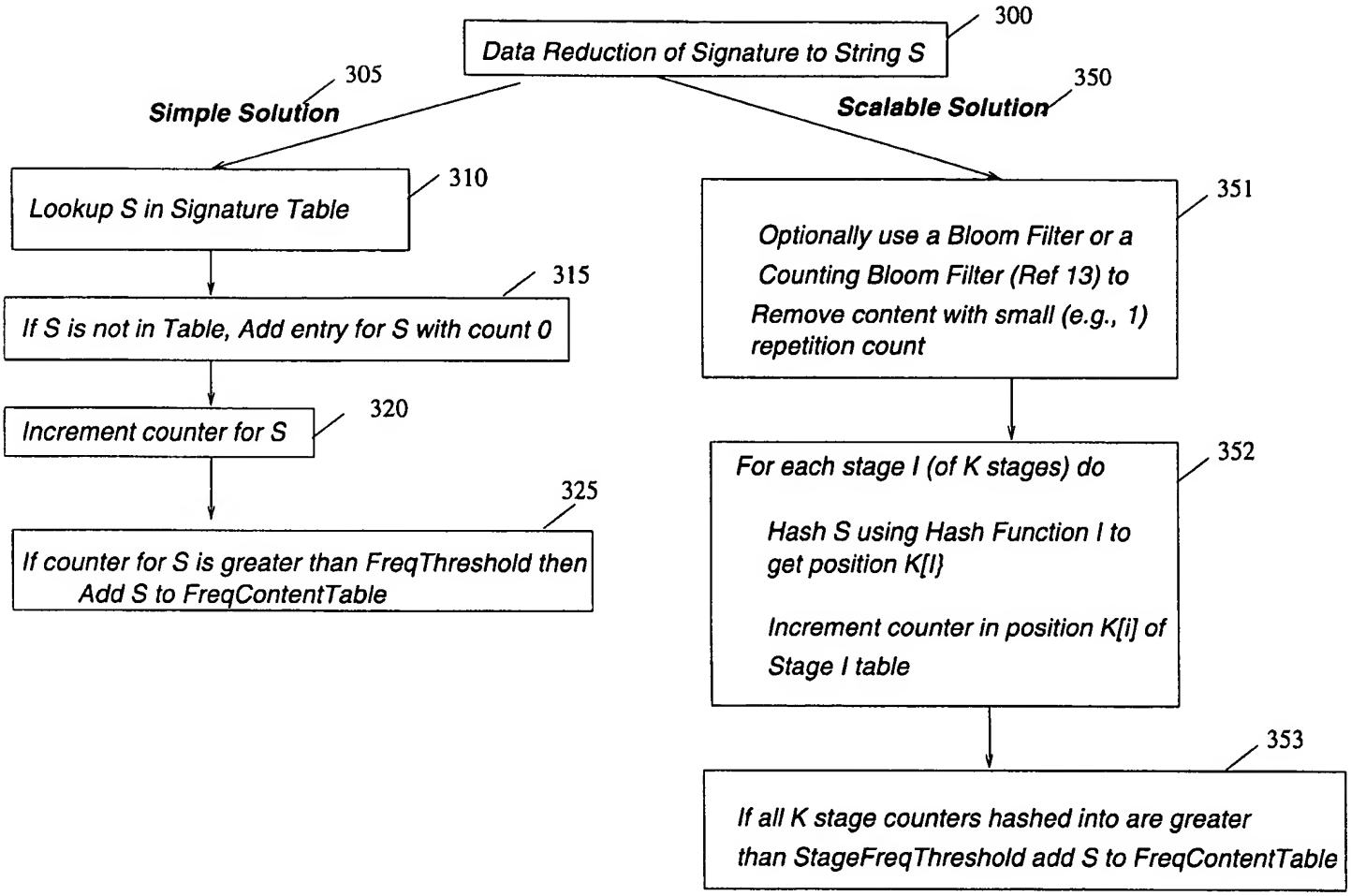

Figure 3: This figure shows the details of Block 215 of the LSIDS system of Figure 2. It sieves out frequent signatures for entry into the FrequentContentTable. Two alternatives are described, a simple version and a scalable version.

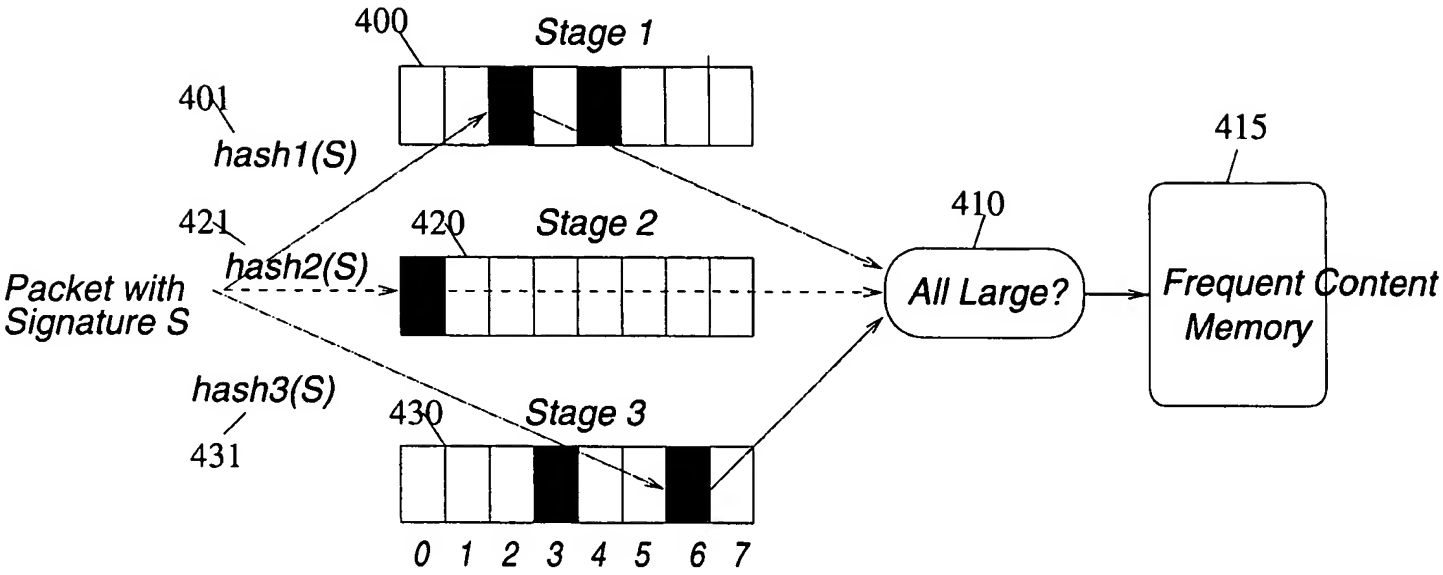

Figure 4: To identify frequent content using only a small amount of memory, a packet with content C is hashed using hash function $hash1$ into a Stage 1 hash table, $hash2$ into a Stage 2 hash table, etc. Each of the hash buckets contain a counter that is incremented by 1. If *all* the hash bucket counters are above the threshold (shown black), then content C is passed to the frequent content table for more careful observation.

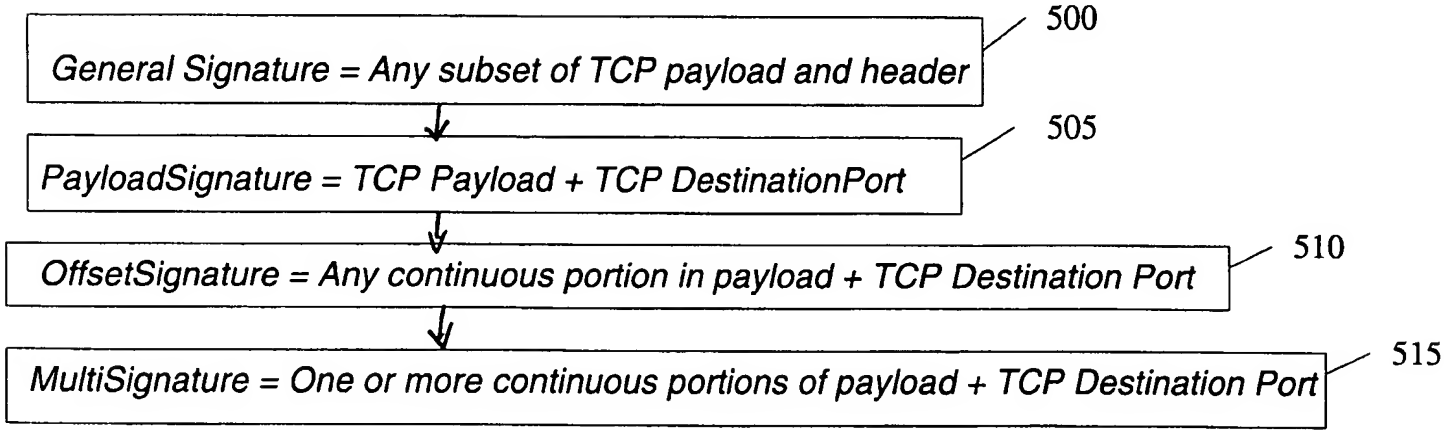

Figure 5: This figure shows the details of Block 205 of the USIDS system of Figure 2.

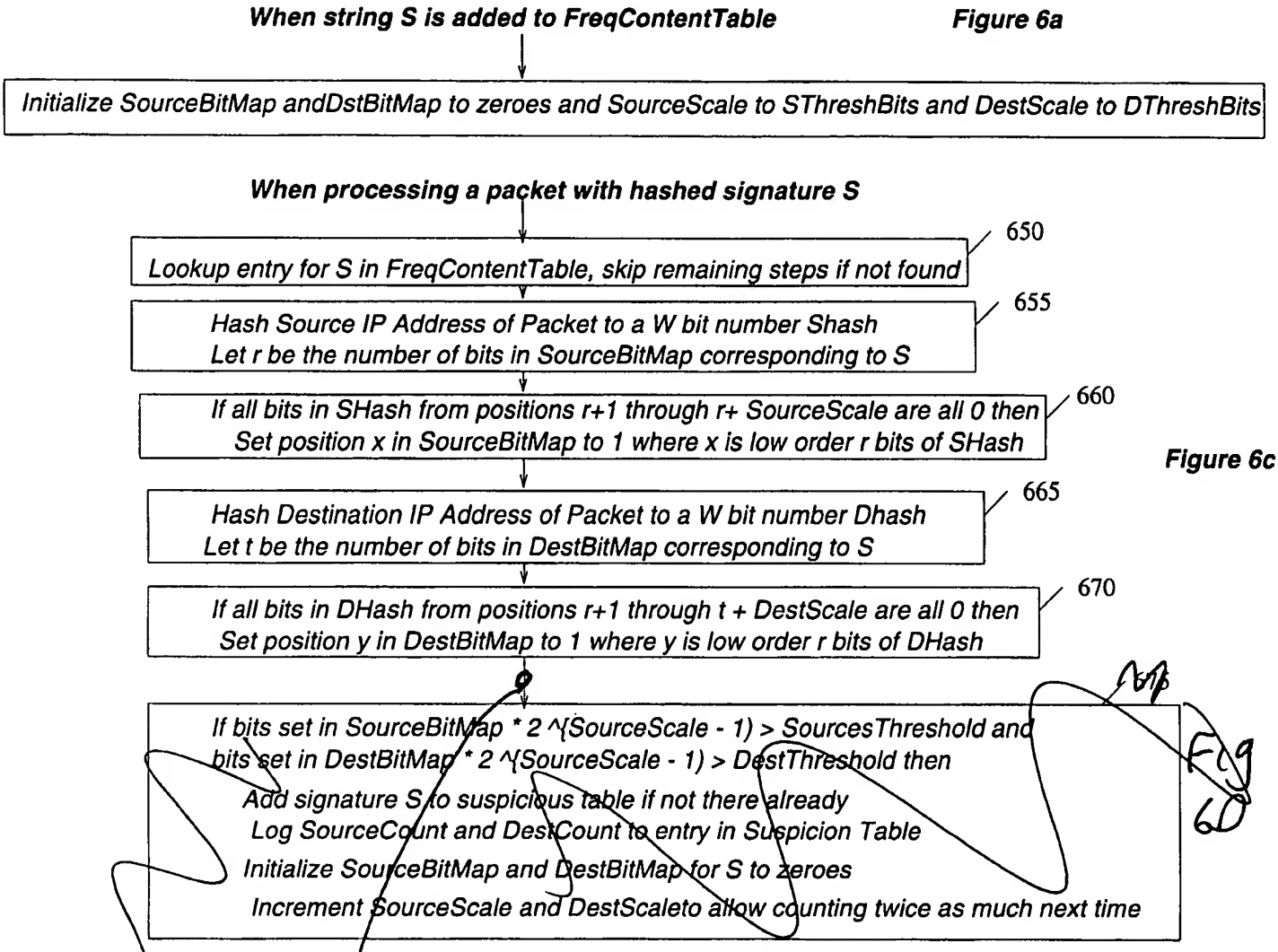

Figure 6: This figure shows the details of block 230 of the USIDS system of Figure 2. It shows how frequent signatures are checked for signs of large scale involvement and rising infection levels. Such signatures are entered in the suspicious signature table and their source count and destination counts are logged to record the progress of the infection.

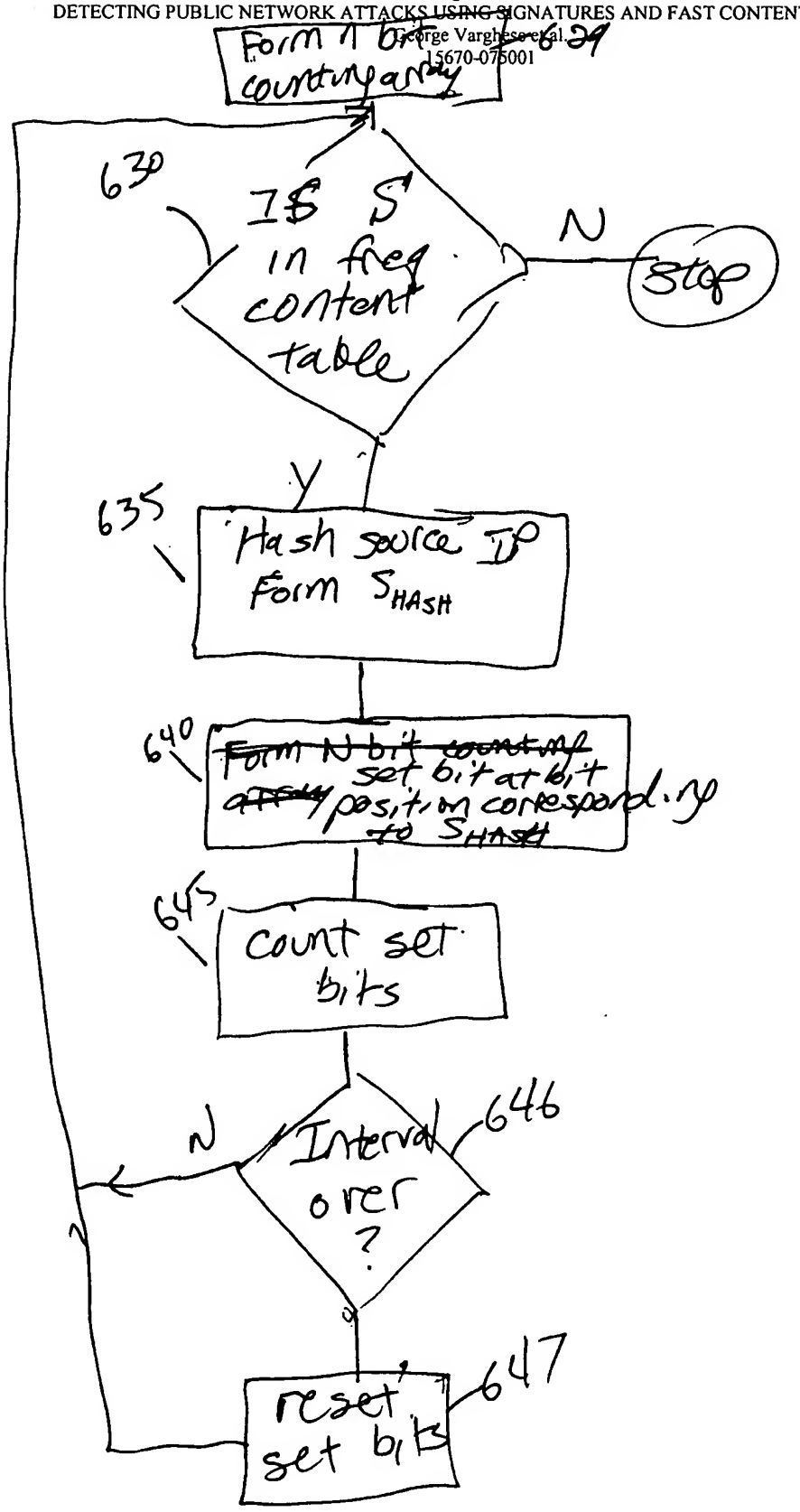
Form 1 bit counting array
630
IS S in freq content table
N
Stop
Y
635
Hash source IP Form S_{HASH}
640
~~Form N bit counting array~~ set bit at bit position corresponding to S_{HASH}
645
count set bits
646
Interval over ?
N
647
reset set bits

FIG 6B

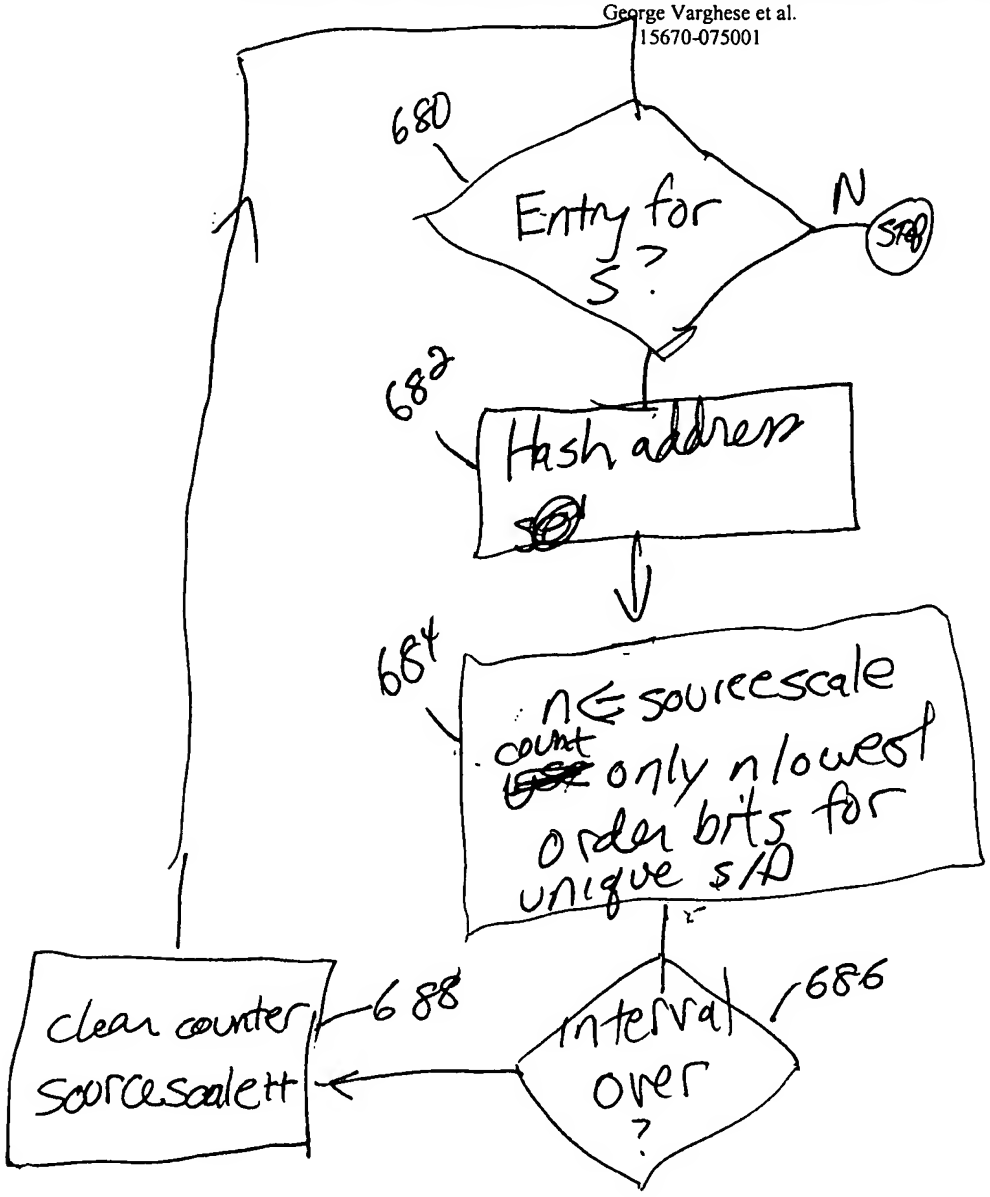
680
Entry for S ?
N
STOP
682
Hash address
684
n ∈ sourcescale
count only n lowest order bits for unique S/D
686
interval over ?
688
clear counter
sourcescale++

FIG 6D

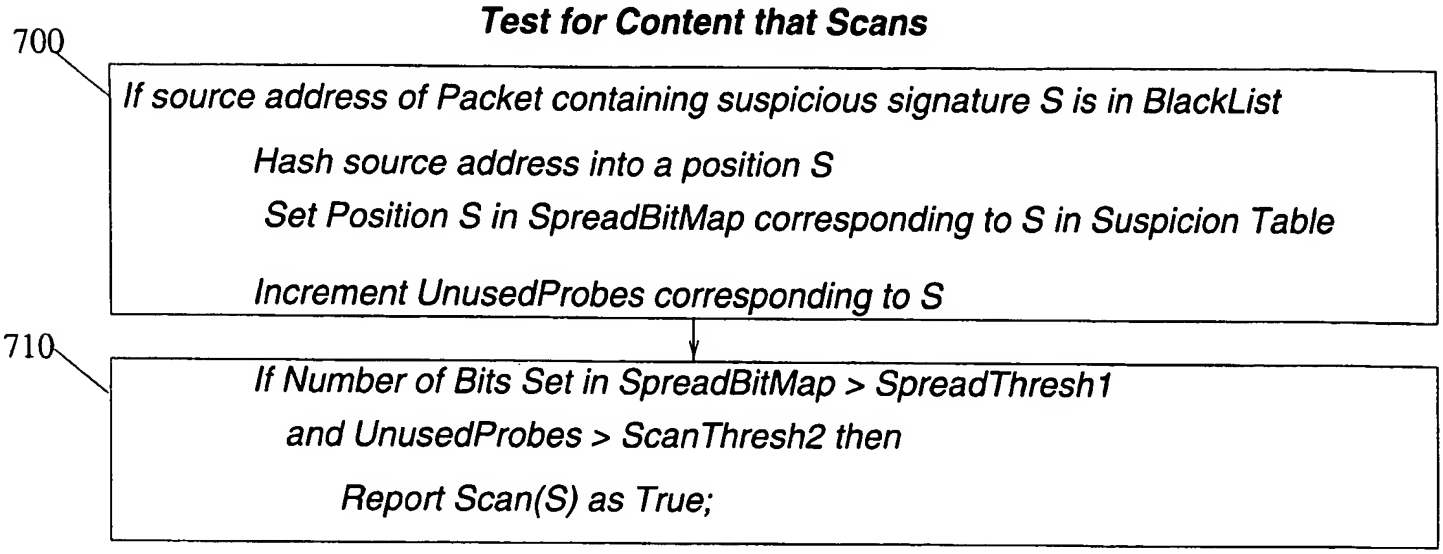

Figure 7: Scan test as part of the further tests (245) of the LSIDS system of Figure 2

Figure 8a

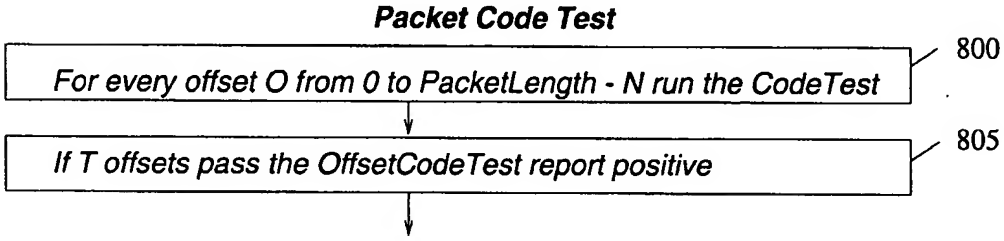

Figure 8b

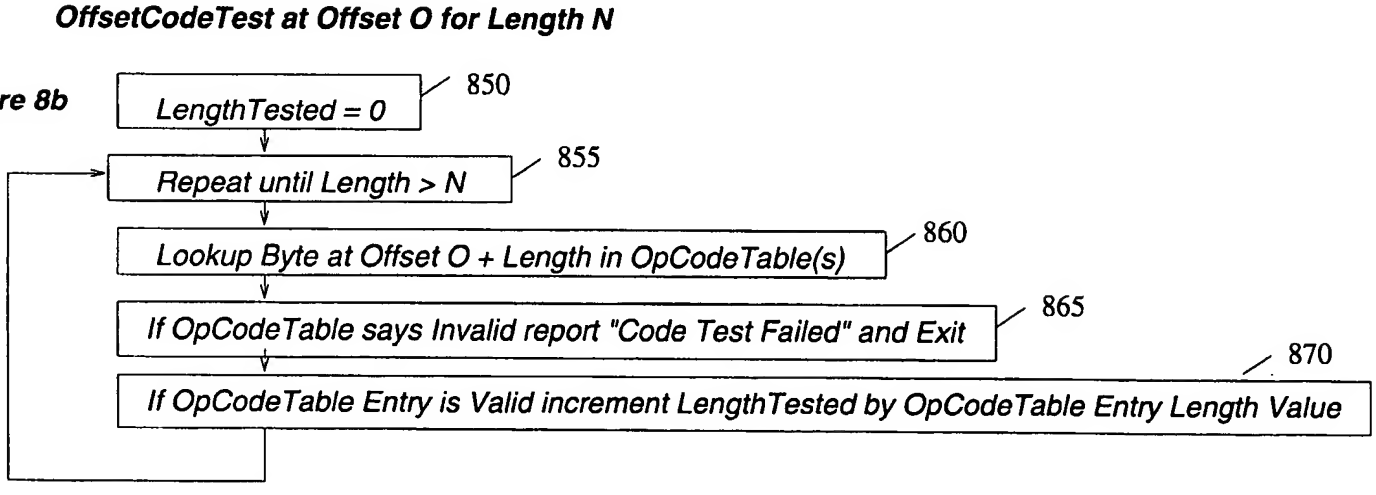

Figure 8: Code test as part of further tests (245) of the LSIDS system of Figure 2

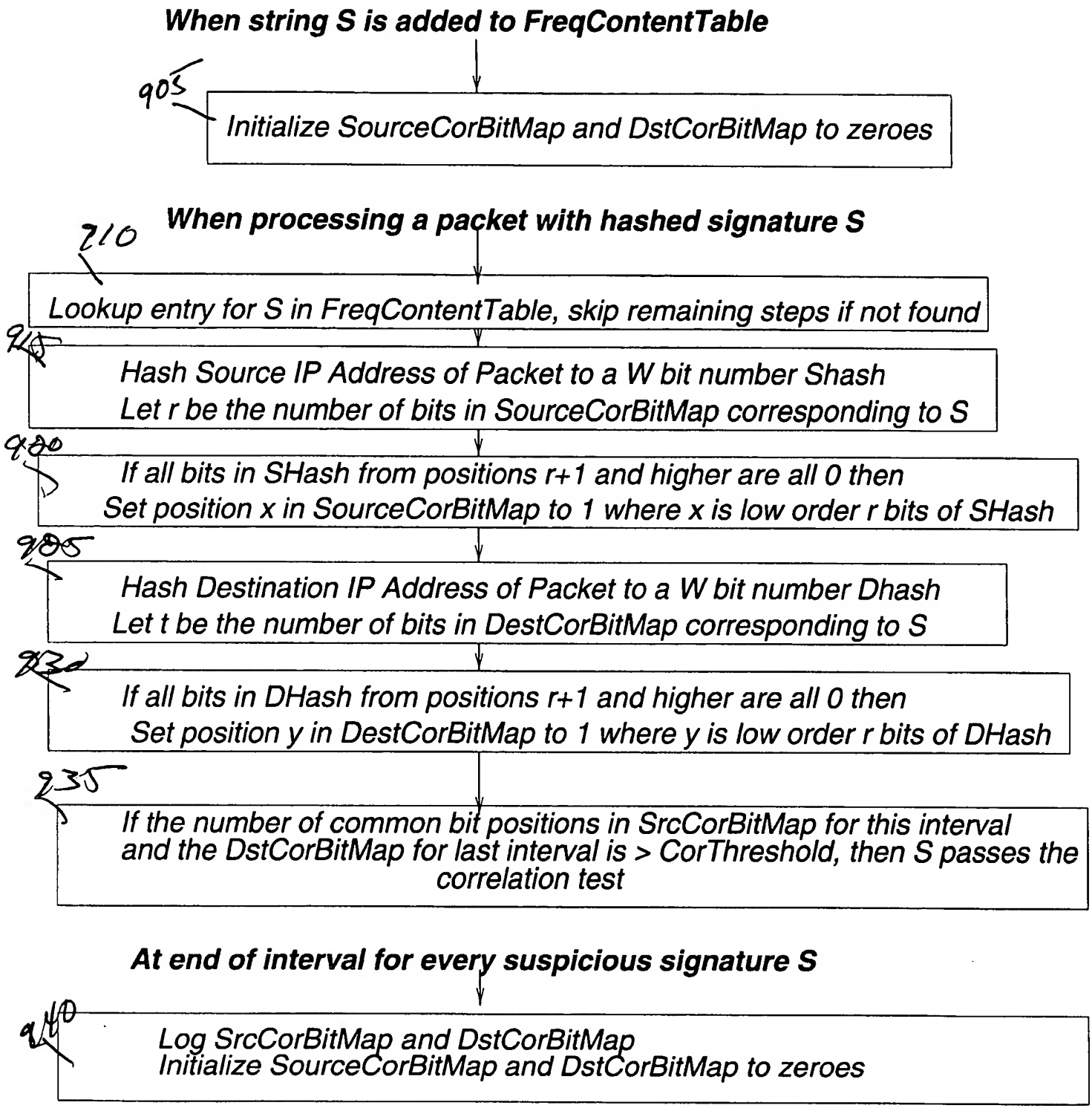

Figure 9: Correlation test as part of the further tests (245) of the USIDS system of Figure 2

If Signature S passes a Bayesian Spam test (an example is in Reference 3) then report that S passes the spam test

Figure 10: Spam test as part of the further tests (245) of the LSIDS system of Figure 2

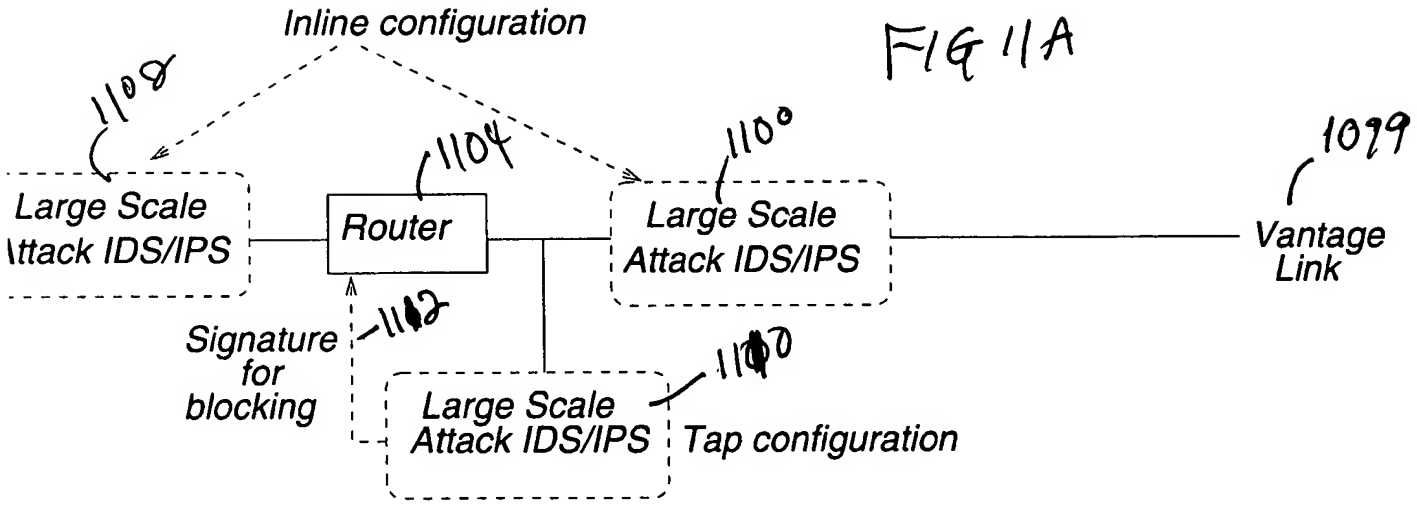

FIG 11A

Sample Intrusion Detection (IDS) and Prevention (IPS) Configurations

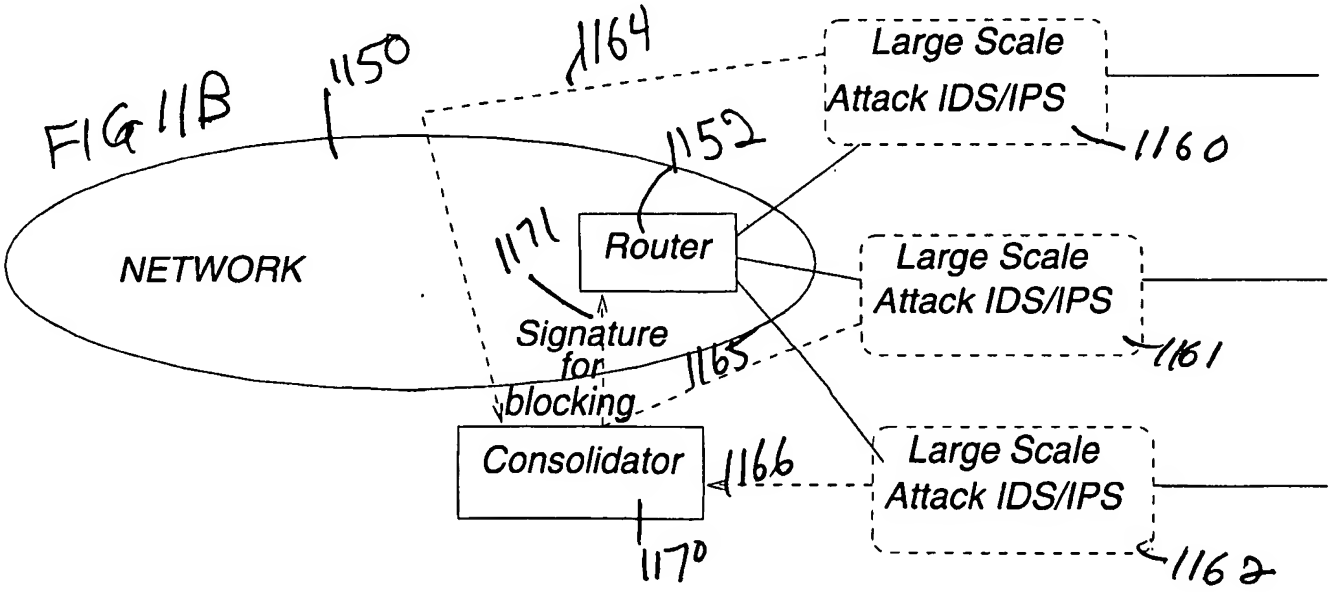

FIG 11B